PATENT
ATTORNEY DOCKET NO. 09669/004001

APPLICATION

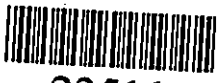
FOR

UNITED STATES LETTERS PATENT

TITLE: **METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS**

APPLICANTS: **Dan BUTNARU and Raphaël ROSSET**

"EXPRESS MAIL" Mailing Label Number: EL656798225US
Date of Deposit: July 17, 2001



22511
PATENT TRADEMARK OFFICE

METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS

The present invention relates to a method for customizing a set of several second security units, comprising secure downloading of an application key from a first security unit to said second security units in said set, wherein said first unit and said second units each comprise at least one memory.

In particular, this invention can advantageously be applied during a phase when second security units are customized in such fields as customer fidelity and banking.

Such a customization method is carried out before said second units are put into use. For example, when they are used in the field of customer fidelity, the second units are found in gas station terminals and are used so as to provide security services in debit-credit transactions of fidelity points between one of said terminals and user credit cards. In the banking field, the second units are found in banking terminals and provide secure services for money transactions in user credit cards.

A well-known state of the art which is disclosed in the published US patent No 5 517 667 under the name of DAQ Electronics, teaches that there exists a key encryption system exists for making secure communications that can be established between a second security unit or "master unit" and a third user unit or "remote unit", when the latter is installed in a remote location, such as a portable telephone. This security system is based on the use of a temporary communication key. According to this system, after the user unit has been installed at its remote location, a communication key is generated by means of the second unit. Accordingly, for establishing each communication from

the second unit to the user unit, the encrypted communication key is sent. The communication key enables exchange of secure messages between the second and user units, as it is only known by these two units. More specifically, the key is based on a pair of secret numbers which are unique to each user unit, and the second unit includes all pairs corresponding to all user units. This system is even more secure as a pair of two secret numbers is written within the user unit's memory, which is volatile. Thus, when a communication is completed and when the user unit is no longer supplied with power, this pair is erased and there is no risk of unauthorized discovery of both secret numbers. In order to establish another communication, the system generates another communication key.

The above-mentioned document describes a system which is put into operation when using a second unit and a user unit with an aim to establish a secure communication between both units by using the same communication key, which is dedicated to communications. It provides no description whatsoever of a customization system for secure key downloading in a set of several second security units.

Therefore, a technical problem to be solved by an object of the present invention is to provide a method for customizing a set of several second security units comprising secure downloading of an application key from a first security unit to said second security units in said set, wherein said first unit and second units each comprise at least one memory, so as to prevent, on the one hand, unauthorized discovery of said application key, and on the other hand, to speed up the customization phase of said second security units.

A solution to the technical problem posed is characterized in that said customization method comprises the steps of :

for each second unit in said set,

- on each downloading, computing, in the first unit, an operation key based on a piece of information specific to the second unit, a transport key, and a diversification algorithm, said transport key residing in the memory of the first security unit, said memory being non-volatile,

- encrypting the application key in the first unit, based on information comprising said operation key and an encryption algorithm, said application key residing in said memory,

- sending data comprising the encrypted application key to the second unit,

- on each downloading, computing, in the second unit, the operation key based on the piece of information specific to the second unit, the transport key and the diversification algorithm, wherein the same transport key resides in the non-volatile memory of each second security unit in said set, said operation key not being stored in the memory of said second unit,

- decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm.

Therefore, as will be seen in detail below, the downloading method of the present invention enables, by computing said operation key and only preserving it for the period when the application key is being encrypted or decrypted, to improve downloading security of an application key. Therefore, a defrauder will neither be able to access said operation key nor, as a consequence, the application key. Possible tampering is therefore prevented and time-consuming operations for the customization phase are no longer carried out, since the computation time of the operation key is negligible with respect to the access time required for storing said key.

The present invention will be understood more fully from the description given herebelow and from the

accompanying drawings which should not be taken to be limiting the invention.

Figure 1 is a view showing a first unit and several second units belonging to the same set.

Figure 2 is a view showing a first unit and a second unit of Figure 1.

Figure 3 is a view showing a data interchange between the first unit and the second unit of Figure 2.

Figure 4 is a view showing a second interchange of data between the first unit and the second unit of Figure 2.

Figure 5 is a view showing a first interchange of data between the first unit and the second unit of Figure 2.

Figure 6 is a view showing a first interchange of data between the first unit and the second unit of Figure 2.

Figure 1 shows a first security unit AS and several security units EI belonging to the same set S (not shown), each of the units (AS, EI) comprising at least one non-volatile memory M. The first unit AS as well as the second units EI of said set S have the same transport key T and the same algorithm ALGO1, referred to as a diversification algorithm, which reside in memory M. Figure 2 shows unit AS as well as one unit EI from the set S. Each second unit EI of set S has the same transport key T. Thus, a set of second units EI is differentiated from another set by means of transport key T. For example, two sets of second units EI correspond to two different gas station providers.

Moreover, the first unit AS has an application key TA and an encryption algorithm ALGO2. It should be noted that both algorithms ALGO1 and ALGO2 may use the same basic algorithm. Each unit EI of said set S comprises specific information SN and at least one user application (not shown) such as an application providing security services for fidelity point debit-credit transactions.

In order to use security units EI of said set S, each second unit EI of said set S must first download an application key TA from the first unit AS, during a so-called customization phase comprising the steps described below. This key is transferred by means of a standard communications network. A defrauder who would spy on said network or said units is prevented from accessing keys in the units as described below.

In a first step, on each downloading, a computation is made in the first unit AS of an operation key T1 based on the information SN specific to second unit EI, transport key T and diversification algorithm ALGO1, said transport key T residing in memory M of first security unit AS, which memory is non-volatile. Preferably, memory M is a rewritable memory. It should be noted that transport key T remains valid even during the phases when the second unit EI is being used, as long as it is not replaced.

Information SN specific to second unit EI does not reside in the first unit. Therefore, as shown in Figure 3, information SN specific to second unit EI is sent to first unit AS before operation key T1 is computed in first unit AS. First unit AS preferably contains several application keys TA. Said key T1 will serve for downloading one of the application key TA contained in first unit AS, and the selected application key will be encrypted and sent to unit EI. One application key is associated with one user application. The appropriate key is chosen according to the application residing in second unit EI.

As shown in Figure 3, for selecting one of said application keys TA, in a second step, a piece of information REF1 relative to application key TA is sent to first unit AS before encrypting application key TA in said unit AS, and the application key TA to be encrypted is chosen based on said information REF1. For example, a reference representing a key number of three can be sent by second unit EI to indicate that the third key, which

corresponds to an application in said unit EI, has been chosen. It is the latter that will be downloaded into second unit EI. If there is no application key TA referred to by said number REF1, the first unit AS indicates that the key does not exist.

In a third step, as shown in Figure 3, application key TA is encrypted in first unit AS from information comprising said operation key T1 and encryption algorithm ALGO2. The operation key temporarily resides in a second volatile memory (not shown) in first unit AS.

In order to protect first unit AS against possible tampering, after application key Ta has been encrypted, the operation key T1 that was temporarily saved within the second volatile memory of first unit AS is erased.

After said key TA has been encrypted, data "DATA" comprising the encrypted application key TA is sent to the second unit TA.

In a fourth step, encrypted application key TA is decrypted in second unit EI based on information including operation key T1 and a decryption algorithm ALGO2P which is the inverse of encryption algorithm ALGO2. In this step, in order to find out the chosen application key TA, it is necessary to use the same operation key T1 as used for encrypting said application key TA in the first security unit AS. For that purpose, before decrypting said encrypted application key TA, on each download, a computation is made in second unit E1 of operation key T1 based on information SN specific to second unit EI, transport key T and diversification algorithm ALGO1, said same transport key T residing in non-volatile memory M of each second security unit EI of said set S, said operation key T1 not being stored within memory M of a second unit EI. Preferably, the memory M of the second unit is rewritable. The operation key T1 is temporarily saved within a second volatile memory (not shown) in second unit EI.

It should be noted that this computation can be done at any time before application key TA is encrypted. The data items required for computing operation key T1 in second security unit EI are the same as those used for computing operation key T1 in first unit AS. Therefore, both keys T1 are identical and the chosen application key TA is indeed found in second unit EI. It was not necessary to send the operation key T1 over the communication network.

In a fifth step, after application key TA has been decrypted and preferably just before this decryption, the temporarily saved operation key T1 is erased from said second volatile memory in second unit EI.

The fact of, on the one hand, not sending any operation key T1 over the communication network and on the other hand, not storing any operation key T1 within a non-volatile memory M in a second module EI and finally, the fact that said operation key only resides in the second unit only for the time required for decrypting application key TA, makes tampering more difficult to carry out inasmuch as, if a defrauder wishes to find an application key TA, he or she should first find the operation key T1 in use. Finally, this facilitates customization and setting up an n-th second unit EI since, for customizing second units, it is no longer required to carry out two downloads, first one for downloading an operation key TA and second, for downloading an application key TA, but downloading only an application key TA is sufficient. Thus, one gets rid of the first downloading operation which is usually carried out by an entity different from first unit AS, which generally complicates things correspondingly.

Just as the first unit AS, a unit EI will preferably comprise several application keys TA. Thus, by means of a second unit EI, several applications can be handled. Moreover, this improves the security of said units since, on the one hand, it will be more difficult for a defrauder to uncover an application key from among

others, and on the other hand, to know to what application it is dedicated to. In the previous example relating to the field of customer fidelity, when using a second unit EI, the latter should be able to provide various services such as securing debit-credit transactions of fidelity points, for example, for different fuel types. Thus, it is important to have different application key TA in unit EI for managing the security of said different transaction types, which represent different applications.

Therefore, in a sixth step, a piece of information REF2 pertaining to an application key TA is sent to second unit EI before said encrypted application key TA is decrypted in unit EI, as shown in Figure 4. Information REF2 enables to either choose application key TA, which will be assigned the value of the application key originating from the first unit AS, or indicate a location where said key TA provided by said first unit AS will be loaded. Therefore, it is possible to either modify a value of a key TA already residing in said second unit EI, or to download a new application key TA into a second unit EI for a new user application.

In case application key TA referred to by said information REF2 does not exist or said location does not exist or is not designed for accepting a key, second unit EI rejects the received key and indicates that an error has occurred. It should be noted that the REF1 and REF2 information sent to the first and second security units, respectively, can be equivalent.

Later on, when used, one of the application keys TA residing in second unit EI can be used by said unit for identifying itself with respect to external entities such as a user card. However, said identification has to be unique. Therefore, key TA should not have any duplicate. Thus, when it is desired to download this key, the chosen application key TA is diversified within unit AS, before said key is encrypted. Diversification

is done as a function of information specific to each second unit.

Finally, in a last step, after said encrypted application key TA has been decrypted, key TA is stored into second unit EI. Storing application key TA in said second unit EI is done based on information REF2 pertaining to an application key TA. The key is stored in rewritable non-volatile memory M.

Second unit EI can now be used and placed at a remote user location such as a gas station terminal. It should be noted that no operation key T1 has been transferred from first unit AS to second unit EI and loaded into memory M of the security modules. The operations required for both of these actions are not performed, which reduces the time needed for customization. Thus, no secret key immediately usable by an algorithm is stored, which prevents unauthorized analysis of said algorithm for uncovering said data. Consequently, it is useless for a defrauder to either spy on the communication network or the security modules in order to find out the operation key T1 used.

Another advantage of the object of the present invention lies in the fact that information SN specific to each second security unit EI is unique. Operation key T1, which has been diversified, i.e. computed based on said information, is therefore unique to each security unit EI. Therefore, encrypted application key TA, which is a function of said operation key T1, is only intended for a single second destination unit EI, which enhances the security feature of this invention. If a second unit EI does not have the same information SN as the one used for computing operation key T1 in first unit AS and if it therefore receives an application key TA which is not intended for it, it rejects this key and indicates that an error has occurred.

Other security features described below are within the scope of the present invention.

The object of the present invention provides an additional step, shown in Figure 4, according to which a random number R obtained from second unit EI is sent to first unit AS before application key TA is encrypted within first unit AS. Information that are useful, on the one hand, to encrypt application key TA in first unit AS, and on the other hand, to decrypt encrypted application key TA within second unit EI, comprise the random number obtained from second unit EI. The use of a random number R for encrypting and decrypting said application key TA avoids having the same encryption value for the same application key TA intended for a second unit EI when, for example, said key is loaded several times into said unit. Thus, each encryption of an application key TA intended for a second unit EI is unique. Therefore, a defrauder who spies on the communication network and gathers data DATA as it is transferred never obtains the same encryption value and therefore cannot uncover any secret relating to the transferred application key TA.

However, during such a transfer, the defrauder may have carried out unauthorized operations which alter the transferred data. Thus, the data DATA, which include the encrypted application key TA, are verified for integrity. For this purpose, as shown in Figure 5, a certificate CAS is computed in first unit AS on said data DATA, before said data is sent, said certificate thereafter being sent later on to the second unit EI and verified within said second unit before encrypted application key TA is decrypted in said second unit EI. In order to carry out verification, certificate CEI is computed in second unit EI based on the received data and both certificates CAS and CEI are compared. If a fraud or an error has occurred during said transfer, the verification of certificate CAS is erroneous, the decryption of application key TA is not performed and second unit EI indicates that an error has occurred. This system therefore guaranties integrity of data DATA

when it is transferred from first unit AS to second unit EI over the communication network, before using a second unit EI, that is before on-site use. Moreover, in case the verification is not valid, this avoids having to carry out an unnecessary decryption and therefore a useless waste of time.

Just as it is necessary to ensure transferred data integrity, authenticity of the data stored into second unit EI should also be guaranteed. Application key TA is thus verified for authenticity. For that purpose, as shown in Figure 5, before application key TA is encrypted, a signature SAS of said key TA is computed within first unit AS, said signature being subsequently sent to second unit EI and verified within said unit. Signature verification of said application key TA is performed after encrypted key TA is decrypted in the second unit EI and before said key within said unit is stored. In order to carry out this verification, a signature SEI is computed with the decrypted application key TA in second unit EI and the two signatures SAS and SEI are compared. When both signatures match, decrypted application key TA is authenticated and stored. In case the application key TA is not authenticated, this key is not stored and the second unit EI indicates that an error has occurred. The above-described system thus makes it possible to verify that the correct chosen application key TA has been recovered in the first unit AS and not some other key. It should be noted that when said signature SAS exists, certificate CAS is also computed as a function of said signature SAS. This signature is part of the data DATA sent during the third step described above.

Sending data such as a certificate or a signature to a security unit relies on operations whose execution time adds up to that of the customization phase. Thus, in order to reduce the number of access operations to the different units and thus, to reduce the customization time, the data set required by a security

unit is sent once by means of a single command. Random number R, number REF1 relating to an application key TA and number SN specific to second unit EI, are sent to first unit AS by means of a first single command EXPORTKEY. In the same way, encrypted application key TA, number REF2 relating to an application key TA, signature SAS, as well as certificate CAS, when they exist, are sent to second unit EI by means of a second single command IMPORTKEY.

The present invention is more particularly applicable in the case when first security unit AS is a smart card. The smart card comprises a plastic card body into which an electronic unit is embedded, which comprises an integrated circuit chip. This chip usually comprises two memories M and a third volatile memory (RAM), wherein first memory M is rewritable (EEPROM) and the second memory is not rewritable (ROM). First memory M comprises all application keys TA and transport key T. The third memory stores operation key T1. The latter only resides in said memory only during encryption or decryption of the application key in a security module. The diversification and encryption algorithms ALGO1 and ALGO2 may reside in the first or second memory M. However, it should be noted that it is not a prerequisite that these algorithms do not have to reside in the smart card. They can be stored in an entity external to said smart card, for example in a central processing unit of a terminal to which said smart card would be connected.

By means of the smart card, it is possible to ensure a better protection of application key TA. In a smart card, contrary to a computer terminal, for example, the keys are unknown to any entity (a terminal, a card administrator, another smart card, etc.) except for the entity issuing said keys. In addition, tampering is more difficult to perform on a smart card than the central processing unit of a terminal, for example. For

the same reasons, the second security unit is a smart card.

It should be noted that an application key TA, as it is stored in a non-volatile memory M, can be used on several occasions where a second unit EI is used, because even when the latter is no longer powered, the key is not erased.